



## SECURITY ADVISORY – Obihai OBi1022 - Remote Code Execution Vulnerability

Advisory Version 1.0

---

DATE PUBLISHED: August 7<sup>th</sup>, 2019

ANY INFORMATION IN THIS ADVISORY IS SUBJECT TO CHANGE.

*Please Note: Poly takes the security of our customers and our products seriously. This is a living document and may be subject to updates. The latest version of this document can be found at the following URL:*

<https://support.polycom.com/content/support/security-center.html>

### Vulnerability Summary

A vulnerability in the web-based management interface of Obihai OBi1022 phones running EX version firmware, up to 5.1.11 on Build: 4858EX.1311, if exploited, could allow an authenticated, remote attacker with admin privileges to execute arbitrary code or cause a denial of service (DoS) condition.

CVE-2019-14259

### Products Affected

This vulnerability affects Obihai OBi1022 phones running EX firmware up to 5.1.11 (Build: 4858EX.1311).

### Solution

Poly has released firmware updates to address this vulnerability.

Products	Fix
OBi1022	Update to to 5.1.11 (Build: 4983EX).

<http://fw.obihai.com/OBiPhone-5-1-11-4983EX.fw>

In addition, as a further mitigation and aligned with standard security best practices, Poly also recommends that customers change the Admin password on the phones from a default or weak password to a strong (minimum 10 character) password. This mitigation limits the ability of the attacker to compromise the phone and is the quickest measure that can be taken to reduce risk.

### Recognition

We would like to thank the independent security researchers **Stephan Huber** and **Philipp Roskosch** from **Fraunhofer SIT** for discovering this vulnerability, alerting us, and for their cooperative disclosure.

## CVSS v3 Base Metrics

To assist our customers in the evaluation of this vulnerability, Polycom uses the Common Vulnerability Scoring System (CVSS). This system provides an open framework for communicating the characteristics and impacts of information technology vulnerabilities that better enable our customers to make informed decisions and assess the impact on their environment.

## Base CVSS v3 Scores

CVE-2019-14259 9.1 (AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H)

For more information on CVSS v3 please see: <https://www.first.org/cvss>

**Severity:** Critical

Rating	Definition
<b>Critical</b>	A vulnerability, which, if exploited would allow malicious code to execute, potentially without a user being aware.
<b>High</b>	A vulnerability, which, if exploited could impact the confidentiality, integrity, or availability of data, or of the integrity or availability of resources.
<b>Medium</b>	A vulnerability that is limited to a significant degree by factors such as default configuration, auditing, or is difficult to exploit.
<b>Low</b>	A vulnerability that has minimal impact to the system and is extremely difficult to exploit.

## Contact

*Any customer using an affected system who is concerned about this vulnerability within their deployment should contact Polycom Technical Support – either call 1-800-POLYCOM or visit:*

<https://support.polycom.com/content/support/security-center.html>

*For the latest information. You might also find value in the high-level security guidance and security news located at:*

<https://support.polycom.com/content/support/security-center.html>

## Revision History

Revision 1.0 - Original publication: August 7<sup>th</sup>, 2019

---



©2019 Plantronics, Inc. All rights reserved.

**Trademarks**

Poly, the propeller design, and the Poly logo are trademarks of Plantronics, Inc. All other trademarks are property of their respective owners. No portion hereof may be reproduced or transmitted in any form or by any means, for any purpose other than the recipient's personal use, without the express written permission of Poly.

**Disclaimer**

While Poly uses reasonable efforts to include accurate and up-to-date information in this document, Poly makes no warranties or representations as to its accuracy. Poly assumes no liability or responsibility for any typographical errors, out of date information, or any errors or omissions in the content of this document. Poly reserves the right to change or update this document at any time. Individuals are solely responsible for verifying that they have and are using the most recent Technical Bulletin.

**Limitation of Liability**

Poly and/or its respective suppliers make no representations about the suitability of the information contained in this document for any purpose. Information is provided "as is" without warranty of any kind and is subject to change without notice. The entire risk arising out of its use remains with the recipient. In no event shall Poly and/or its respective suppliers be liable for any direct, consequential, incidental, special, punitive or other damages whatsoever (including without limitation, damages for loss of business profits, business interruption, or loss of business information), even if Poly has been advised of the possibility of such damages.

